

UNITED STATES DISTRICT COURT

for the
Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

BLACK APPLE IPHONE 15 PLUS, WITH SERIAL
NUMBER GVQM629N7W, DESCRIBED IN
ATTACHMENT A

Case No. **5:24-mj-352 (MJK)**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sections 2252A(a)(1) and (a)(5)(B)	Transportation and possession of child pornography

The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Cory R Shepard

Applicant's signature

Cory Shepard, Task Force Officer, HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: **8/4/2024**

Mitchell J Katz

Judge's signature

City and state: **Syracuse, NY**

Hon. Mitchell J. Katz, U.S. Magistrate Judge

Printed name and title

Print

Save As...

Attach

Reset

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Cory Shepard, being duly sworn, hereby state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B

2. I am a Customs and Border Protection Officer (CBPO) with the U.S. Department of Homeland Security (DHS), Customs and Border Protection (CBP), and as such I am empowered by law to investigate and make arrest for offenses enumerated in Title 18, United States Code, Section 2252A.

3. I have been employed as a Task Force Officer (TFO) since November 2020 and I am currently assigned to the Homeland Security Investigations (HSI) Task Force Resident Agency Office in Alexandria Bay, New York. While assigned to HSI, I have been responsible for enforcing customs laws, immigration laws and federal criminal statutes of the United States. My responsibilities as a TFO with HSI include, but are not limited to, conducting investigations, executing arrest warrants, executing search warrants, collecting evidence, and interviewing witnesses. I have been a TFO for approximately three and one-half years and have investigated and/or participated in investigations of child pornography, narcotics, smuggling, and immigration offenses. My duties include the enforcement of federal criminal statutes involving the sexual exploitation of children, as codified in Title 18, United States Code, Sections 2251 through 2259. I have participated in searches of premises and assisted in gathering evidence by means of a search warrant. I have received training in the area of the importation and distribution of child pornography and have had the

opportunity to observe and review numerous examples of child pornography in many forms, including video and computer media.

4. The statements contained in this affidavit are based upon my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, and information provided to me by other law enforcement officers. I have not set forth every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence of violations of Title 18, United States Code, Sections 2252A(a)(1) and (a)(5)(B) (transportation and possession of child pornography) are presently located in the **Subject Device**.

THE SUBJECT DEVICE TO BE EXAMINED

5. The property to be searched is an Apple iPhone 15 Plus with serial number GVQM629N7W, described further in Attachment A (the **Subject Device**). The **Subject Device** is currently located at 46735 Interstate Route 81, Alexandria Bay, New York.

6. The applied-for warrant would authorize the forensic examination of the **Subject Device** for the purpose of identifying electronically stored data particularly described in Attachment B.

FACTS SUPPORTING PROBABLE CAUSE

7. On or about August 3, 2024, at approximately 10:39 p.m., Rylin TURLEY entered the United States from Canada through the Alexandria Bay, NY Port of Entry. TURLEY was traveling in a vehicle with three other individuals. Officers with U.S. Customs and Border Protection (CBP) referred TURLEY for a secondary inspection.

8. As part of that secondary inspection, TURLEY was found in possession of an iPhone on his person (the **Subject Device**). TURLEY provided an officer with the access code. A CBP officer manually reviewed the **Subject Device**.¹

9. During that review, a supervisory CBP officer looked in the Photos App of the **Subject Device**. Within that app, the officer navigated to “Recently Deleted” items. There, the officer observed a video² that depicted an adult male penis penetrating a female child approximately 10 years of age. Upon observing this video, CBP notified HSI for further investigation.

10. I reported to the port of entry to assist the investigation. I also performed a manual review of the **Subject Device**. First, I confirmed the content of the video described in the previous paragraph, which was initially observed by the CBP officer. Next, I looked in other places on the phone that might contain media files.

11. One of the locations I reviewed was a storage app on the phone (App A). According to the Apple app store listing for this program, it is “[t]he best app to protect and hide your private photos & videos. Over millions of people trust [App A] to keep their photos & videos hidden.” Based on my training and experience in other investigations, I know that individuals engaged in the possession, receipt, and transportation of child sexual abuse material (CSAM) use App A and similar apps to store and hide CSAM.

12. Within App A, I observed multiple videos and images that contained CSAM. For example:

¹ A manual review of a phone involves browsing the content on the device itself, as the user would, rather than completing a forensic extraction of the data for review on a different device.

² This file and the others described in this affidavit will be made available for the Court’s inspection upon request.

a. One video, labeled 469 of 558, located in the “main” folder, is approximately 18 minutes 57 seconds in length. This video depicts an adult male who penetrates the naked vagina of a prepubescent female child approximately 6 to 8 years old, both digitally and with his penis.

b. Another video file, labeled 525 of 558, depicts the vagina of a prepubescent female child approximately 8 years old being penetrated by an adult male penis. The adult male can also be seen choking the female child with his hand.

7. TURLEY was advised of his *Miranda* rights and subsequently agreed to speak further with interviewing agents. The interview was audio and video recorded. During the interview, in sum and substance:

a. TURLEY acknowledged receiving child pornography material on a social media messaging app (App B), approximately two or three months ago. TURLEY stated that he downloaded the material on the app during a single use.

b. TURLEY stated that after he downloaded the files from App B, he saved it to an account he has with App C.³ He said that he then deleted App B because he “didn’t want to be part of their group anymore [the chat group from which he downloaded the CSAM files]⁴ . . . to be done with it and try to not get in trouble.” TURLEY stated that he transferred the files to App C so he could still have access to the materials.

³ The Apple app store listing for App C describes the program as follows: “[App C] provides user-controlled encrypted cloud storage that’s accessed with web browsers and dedicated apps for mobile devices. Unlike other cloud storage providers, your data is encrypted and decrypted by your client devices only and never by us [App C employees].”

⁴ Where applicable to explain and add context to statements, I included my interpretation in brackets. That interpretation is based on my training, experience, and knowledge of the investigation, including my preliminary review of the **Subject Device** and my interview of TURLEY.

c. TURLEY stated that there “may be” files that he downloaded from App B as mentioned above, also stored within App A on his phone.

d. TURLEY indicated that he was attracted to the material downloaded from App B.

13. The **Subject Device** is currently in the lawful possession of HSI. It came into HSI’s possession in the following way: a border search was performed on the **Subject Device** as its owner, TURLEY, transported it across the border from Canada into the United States on or about August 3, 2024, and contraband (namely, CSAM) was observed on the device, and it was seized. Therefore, while HSI might already have all necessary authority to examine the **Subject Device**, I seek this additional warrant out of an abundance of caution to be certain that an examination of the **Subject Device** will comply with the Fourth Amendment and other applicable laws.

14. The Device is currently in storage at 46735 Interstate Route 81, Alexandria Bay, New York. In my training and experience, I know that the **Subject Device** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **Subject Device** first came into the possession of HSI.

DEFINITIONS

15. The following definitions apply to this affidavit its attachments:

a. “Child Erotica” means materials or other items that are sexually arousing to persons having a sexual interest or desire in minors, but that are not necessarily, in and of themselves, obscene, or that do not necessarily depict minors in sexually explicit poses or body positions.

b. “Child Pornography” and “Child Sexual Abuse Material” (CSAM) includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).

d. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

e. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices

(including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware.

g. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

i. “Minor” means any person under the age of 18 years. See 18 U.S.C. § 2256(1).

j. “Sexually explicit conduct” applies to the visual depictions that involve the use of a minor, see 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, see 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated: (a) sexual intercourse (including genital-

genital, anal-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. See 18 U.S.C. § 2256(2)(A).

k. “Visual depictions” include undeveloped film and videotape, as well as data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

l. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.

BACKGROUND ON ELECTRONIC DEVICES AND CHILD PORNOGRAPHY

16. Based on my knowledge, training, and experience, and the experience and training of other law enforcement agents and investigators with whom I have had discussions, I know that electronic devices, including cellular telephones serve different roles or functions with respect to possession of child pornography.

17. An electronic device's ability to store images in digital form makes the cellular telephone itself an ideal repository for child pornography. The size of the electronic storage media used in cellular telephones has grown tremendously within the last several years and can store literally thousands of images at very high resolution.

18. As with most digital technology, communications made from a cellular telephone are often saved or stored on that device's hard drive or memory card. Storing this information can be intentional, for example, by saving an e-mail as a file, or saving the location of a favorite website in "bookmarked" files. Digital information, however, can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, users' Internet activities generally leave traces that a trained digital forensic examiner often can recover, including evidence and other items that show whether a cellular telephone was sharing data files, and some of the data files that were uploaded, downloaded, and transferred. Such information is often maintained indefinitely until overwritten by other data.

19. Modern technology in the past several years has transformed the cellular telephone from a simple mobile telephone device into a mobile mini-computer commonly referred to as a "smart phone," capable of Internet access through wireless internet connections as well as cellular telephone signals. Built in digital camera and video camera capabilities are common features, and video and image storage capabilities can hold thousands of images and hours of video files. By being able to access the Internet virtually anywhere, digital images and videos taken with a cellular telephone and stored on the cellular telephone can be shared with others by e-mail (phone to computer), text messaging (phone to phone), or uploaded to and displayed on Internet websites. Smart phones generally have

global positioning satellite (GPS) capabilities that allow the cellular telephone to provide driving directions and include GPS coordinates in such features as sharing locations on social networking websites and imbedding into the metadata of photographic images the coordinates of where an image was taken.

COLLECTORS OF CHILD PORNOGRAPHY

20. Individuals who are interested in child pornography may want to keep the child pornography files they create or receive for additional viewing in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy of their homes, on cellular telephones, or in other secure locations. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished fantasies, the collector rarely, if ever, disposes of his collection. The collection may be culled and refined, but, over time, the size of the collection tends to increase. Individuals who utilize a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to part with them over time.

21. Individuals who collect child pornography may search for and seek out other like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact may also help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: text messages, video messages, electronic mail, email, bulletin boards, IRC, chat rooms, newsgroups, and instant messaging.

22. Individuals who collect child pornography may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings, and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

23. Individuals who collect child pornography may keep names, electronic mail addresses, cellular and telephone numbers, or lists of persons who have shared, advertised, or otherwise made known their interest in child pornography or sexual activity with minor children. These contacts may be maintained as a means of personal referral, exchange, and/or commercial profit. This information may be maintained in the original medium from which it was derived.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

8. I am familiar with electronic evidence recovery and have spoken with law enforcement investigators who are trained in computer and cellular telephone evidence recovery. These investigators have extensive knowledge about the operation of cellular telephones and computer systems, including the correct procedures for the seizure and analysis of these systems.

9. Based on my knowledge, training, and experience, I am aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, transferred, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost to the user. Even when files have been deleted, they can be recovered months or years later using specialized forensic tools. This is so because when a person “deletes” a file on a

computer or cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

10. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space located on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data or process in a “swap” or “recovery” file.

11. Apart from user-generated files, an electronic device may contain electronic evidence of how it was used, what it was used for, and more importantly, who used it recently and in the past. This evidence can take the form of operating system configurations, artifacts from operating system or different application operation, file system data structures, and the virtual memory “swap” or paging files. Similarly, files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache” located on the computer. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

12. Although some of the information called for by this search warrant might be found in the form of user-generated documents (such as photographic images and video files), smart phone style cellular telephones can contain other forms of electronic evidence as well:

a. Forensic evidence of how the **Subject Device** was used, the purpose of its use, who used it, and when, is called for under this request for a search warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Computer file systems can record information about the dates and times files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence or physical location. For example, registry information, configuration files, user profiles, e-mail address books, “chats,” instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates and times) may in and of themselves be evidence of who used or controlled the computer or storage medium at a relevant time in question.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw logical conclusions about how it was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team and passed along to the case agents and investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the

nature of the evidence described in Attachment B also falls within the scope of the search warrant.

e. Searching storage media for the evidence described in the Attachment B may require a range of data analysis techniques. It is possible that the storage media will contain files and information that are not called for by the search warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the search warrant is immediately apparent. In most cases, however, such techniques may not yield the evidence described in the search warrant. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. As explained above, because the search warrant calls for records of how the **Subject Device** was used, what it was used for, and who used it, it is likely that it will be necessary to thoroughly search the device to obtain evidence including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a search warrant, a search the **Subject Device** for the things described in this search warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this search warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

13. The search procedure of electronic and digital data contained in cellular telephones, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such cellular telephone and its memory storage device to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents and scanning storage areas;

e. performing key word searches to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

f. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

24. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

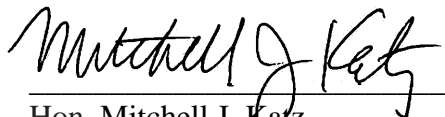
25. Based on the above information, I believe that there is probable cause that contraband and evidence of violations of Title 18, United States Code, Sections 2252A(a)(1) and (a)(5)(B) (transportation and possession of child pornography), as described in Attachment B, will be found on the **Subject Device**, described further in Attachment A. Therefore, based upon the information contained in this affidavit, I request that this Court issue the requested search warrant authorizing the search of the contents of the **Subject Device** described in Attachment A for the items more particularly described in Attachment B.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE.



Cory Shepard, Task Force Officer
Homeland Security Investigations

I, the Honorable Mitchell J. Katz, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on August 4, 2024, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.



Hon. Mitchell J. Katz
United States Magistrate Judge

ATTACHMENT A

Description of Property To Be Searched

The **Subject Device** to be searched is a black Apple iPhone 15 Plus, with serial number GVQM629N7W. The **Subject Device** is currently located at the HSI Resident Agency located at 46735 Interstate Route 81, Alexandria Bay, New York. An image of the **Subject Device** is below.



ATTACHMENT B

Items To Be Seized

1. Items and information that constitute contraband and evidence of violations of Title 18, United States Code, Sections 2252A(a)(1) and (a)(5)(B) (transportation and possession of child pornography), since approximately March 2024, including:

a. Any and all visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

b. Records of the location of the **Subject Device**.

c. Records, including logs and other transaction history, related to the download, receipt, upload, duplication, and transfer of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

d. Internet history including evidence of visits to websites that offer visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256.

e. Correspondence or other documentation identifying persons transmitting through interstate or foreign commerce, including by mail or computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

f. Computer records and evidence identifying who the particular user was who produced, downloaded or possessed any child pornography found on any computer or computer media.

g. Correspondence and other matter pertaining to the production, purchase, possession, receipt or distribution of visual depictions of minors engaged in

sexually explicit conduct as defined in Title 18 United States Code, Section 2256, and evidence that would assist in identifying any victims of the above-referenced criminal offenses, including address books, names, and lists of names and addresses of minors, or other information pertinent to identifying any minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

h. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes evidencing an interest in unlawful sexual contact with children, and evidence assisting authorities in identifying any such children.

i. Any and all records or communications evidencing an intent, or conspiracy, or plan to engage in sexually explicit conduct with a child.

j. Any and all records or communications with minor children, or with persons purporting to be minors.

k. Any and all electronically stored records reflecting personal contact with minors.

l. Any notes, writings or other evidence that would assist law enforcement in identifying victims of sexual exploitation, witnesses thereto, or other subjects that may have assisted, conspired, or agreed to participate in the sexual exploitation of children.

m. Records showing the use or ownership of Internet accounts, including evidence of Internet user names, screen names or other Internet user identification.

n. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related

components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

o. Computer-related documentation that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

p. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records.

q. Documents and records regarding the ownership and/or possession of electronic media being searched.

2. Evidence of user attribution showing who used or owned the **Subject Device** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The authorization to search includes the search of the **Subject Device** listed on the face of the warrant, for electronic data to include deleted data, remnant data and slack space.